JP2000174746A METHOD AND DEVICE FOR DECIPHERING DATA

Bibliography

DWPI Title

Data decoding method involves encrypting K pieces which are selected from divided secret key using disclosure key by preset specification which is stored in memory

Original Title

METHOD AND DEVICE FOR DECIPHERING DATA

Assignee/Applicant

Standardized: **HITACHI SOFTWARE ENG**
Original: HITACHI SOFTWARE ENG CO LTD

Inventor

SAMEJIMA YOSHIKI; MIYAZAKI HIROSHI; TODA JUNICHI

Publication Date (Kind Code)

2000-06-23 (A)

Application Number / Date

JP1999267988A / 1999-09-22

Priority Number / Date / Country

JP1998278012A / 1998-09-30 / JP
JP1999267988A / 1999-09-22 / JP

Abstract

PROBLEM TO BE SOLVED: To decipher data or file enciphered with a public key without knowing a secret key itself and to facilitate the management of divided keys as well by dividing the secret key with a stored primary expression and deciphering the data enciphered with the public key while using divided keys.
SOLUTION: A computer 101 enciphers and preserves a document or file prepared by a user. A key generating means 102 generates the key pair of cipher to be used for the users of plural user computers 101, namely, the public key and secret key of public key cipher. The generated key pair is sent to the user computer 101 and the secret key is divided and sent to divided key holding computers 103. N pieces of divided key holding computers 103 are installed, for example, and hold the divided secret keys of the user. A data deciphering device 104 extracts information concerning the desired enciphered document to be deciphered from the user computer 101 and collects partially deciphered information from K (K

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－174746
（P2000－174746A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ	9/00	６０１Ａ
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ	1/00	６２０Ｚ
		Ｈ０４Ｌ	9/00	６０１Ｆ

審査請求　有　　請求項の数６　ＯＬ　（全 19 頁）

(21)出願番号　特願平11－267988

(22)出願日　平成11年９月22日(1999.9.22)

(31)優先権主張番号　特願平10－278012
(32)優先日　平成10年９月30日(1998.9.30)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　鮫島　吉喜
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　データ復号方法および装置

(57)【要約】
【課題】　秘密鍵自体を知られること無く、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータを復号でき、かつその分割鍵の管理も容易にする。
【解決手段】　公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵がＮ個（Ｎ≧２の整数）に分割され、それぞれをＮ人の分割鍵保有者に保有させ、Ｎ人のうちＫ（Ｋ＜Ｎ）人が保有する秘密鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号する場合に、前記分割鍵保有者の数Ｎに１を加えた数の変数を含む複数の一次式で、１つの変数の係数は常に０でなく、残りＮ個の変数の係数のうちＫ個が０でない複数の一次式を利用して秘密鍵をＮ個に分割し、その分割されたＮ個の秘密鍵のうちＫ個を用いて前記公開鍵で暗号化したデータを復号する。

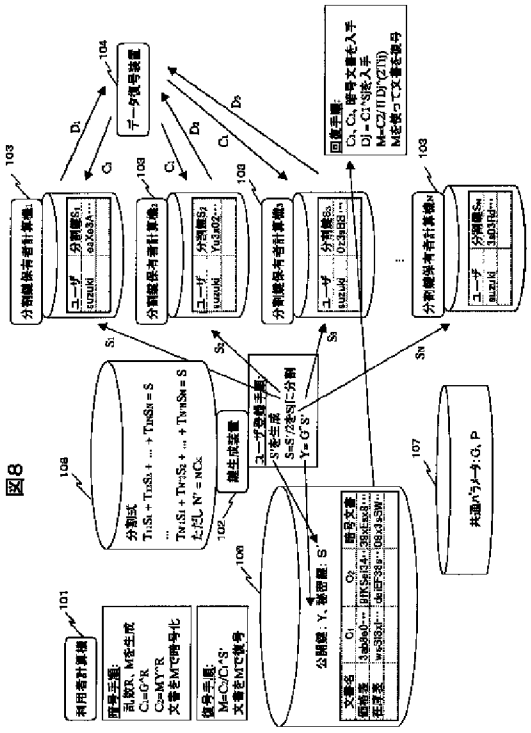


図8

【特許請求の範囲】

【請求項１】　公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をＮ個（Ｎ≧２の整数）に分割し、それぞれの分割鍵をＮ人の分割鍵保有者に割り当てた際の分割鍵保有者の数Ｎに１を加えた数の変数を含む複数の一次式で、かつ１つの変数の係数は常に０でなく、残りＮ個の変数における係数のうちＫ個が０でない複数の一次式を予め記憶した記憶手段を備え、前記Ｎ人のうちＫ（Ｋ＜Ｎ）人に割り当てた分割鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号するデータ復号方法であって、

前記秘密鍵を分割する際に、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵をＮ個に分割し、その分割されたＮ個の分割鍵のうちＫ個を当該分割鍵の保有者から入力させて前記公開鍵で暗号化したデータを復号することを特徴とするデータ復号方法。

【請求項２】　請求項１記載のデータ復号方法において、前記秘密鍵をN_G個（Ｎ≧Ｇ≧２の整数）に分割し、それぞれの分割鍵をＮ人の分割鍵保有者をグループ化したN_G個のグループに割り当て、さらにそれぞれのグループにおいて該分割鍵を各グループの所属人数N_i個（ｉ≧１の整数）に分割し、それぞれをN_i人の分割鍵保有者に割り当て、N_i人のうちK_i人（$N_i \geqq K_i \geqq 1$の整数）の協力が成立したK_G個のグループが協力して前記公開鍵で暗号化されたデータをコンピュータにより復号する場合において、

分割鍵保有者のグループ数N_Gに１を加えた数の変数を含む複数の一次式で、１つの変数の係数は常に０でなく、残りN_G個の変数の係数のうちK_G個が０でない複数の一次式であり、さらに該残りN_G個のそれぞれの変数は、その変数自身とN_i個の変数を含む複数の一次式で表され、その変数自身の係数は０でない共通の値であり、残りN_i個の変数の係数のうちK_i個が０でない一次式を前記記憶手段に予め記憶させるステップと、

前記秘密鍵を分割する際に、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵をN_i個に分割するステップと、

分割されたN_i個の秘密鍵のうちK_i人が入力したK_G個の秘密鍵を用いて前記公開鍵で暗号したデータを復号するステップとを有することを特徴とするデータ復号方法。

【請求項３】　請求項２記載のデータ復号方法において、

Ｎ人の分割鍵保有者のうち、協力が必須となる分割鍵保有者がN_A人いる場合に、該必須分割鍵保有者を唯一の所属構成員とするN_A個のグループと、残りのＮ－N_A人を所属者構成員としてそのうちＫ－N_A人の協力が必要となるグループに分け、さらにこれらN_A＋１個のグループ全部が協力して前記公開鍵で暗号化されたデータを復号する場合において、

前記N_A＋１個のグループ全部が必要となる一次式を生成し、その生成した一次式を用いて前記秘密鍵を分割してＮ人の分割鍵保有者に割り当て、割り当てた秘密鍵を用いて前記公開鍵で暗号したデータを復号することを特徴とするデータ復号方法。

【請求項４】　公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をＮ個（Ｎ≧２の整数）に分割し、それぞれの分割鍵をＮ人の分割鍵保有者に割り当て、Ｎ人のうちＫ（Ｋ＜Ｎ）人に割り当てた分割鍵を用いて前記公開鍵で暗号化されたデータを復号するデータ復号装置であって、

前記分割鍵保有者の数Ｎに１を加えた数の変数を含む複数の一次式で、かつ１つの変数の係数は常に０でなく、残りＮ個の変数における係数のうちＫ個が０でない複数の一次式を予め記憶した記憶手段と、

前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵をＮ個に分割し、その分割されたＮ個の分割鍵をＮ人の分割鍵保有者に割り当てる鍵生成手段と、

Ｎ人の分割鍵保有者に割り当てたＮ個の分割鍵のうちＫ個を当該分割鍵の保有者から入力させる入力手段と、

入力されたＫ個の分割鍵を用いて前記公開鍵で暗号化したデータを復号する復号手段とを備えることを特徴とするデータ復号装置。

【請求項５】　暗号化されたデータの復号開始時に、復号に必要な分割鍵の数または分割鍵保有者数を表示する表示手段をさらに備えることを特徴とする請求項４記載のデータ復号装置。

【請求項６】　Ｎ人の分割鍵保有者に割り当てる分割鍵は、携帯可能な記録媒体に格納して各分割鍵保有者に保有させることを特徴とする請求項４または５記載のデータ復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をＮ個（Ｎ≧２の整数）に分割し、それぞれをＮ人の分割鍵保有者に保有させ、Ｎ人のうちＫ（Ｋ＜Ｎ）人が保有する秘密鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号するデータ復号方法および装置に関し、例えば、企業内で担当者が作成、暗号化した文書を、その担当者が不在の時に復号する必要が生じた場合に、担当者の上長や所属のコンピュータ管理者が協力し、あるいはさらに特定の誰かによる協力を受けて復号する場合のデータ復号方法および装置に関するものである。

【０００２】

【従来の技術】従来において、複数人の分割鍵保有者に預けた秘密鍵を用いて、該秘密鍵に対応する公開鍵で暗号化したデータを復号する方法として、Shamir（A.Shamir、”How to share a secret″、Communication of ACM

22（11)、612-613、1979年11月号)の方法がある。この方法では、秘密鍵の情報をＮ人（Ｎ≧２の整数）の分割鍵保有者に分割して渡し、そのうちＫ人（Ｋ≦Ｎ）が保有する分割秘密鍵を集めることにより秘密鍵自体を復元し、その復元した秘密鍵によって、暗号化したデータを復号化可能にしたものである。

【０００３】一方、暗号通信を不正目的に利用しているユーザの通信内容を解読して犯罪捜査に利用する方法として、暗号文の復号鍵を供託機関に登録しておいて、捜査が必要な場合に捜査機関が裁判所の許可を受け、復号鍵を供託機関から入手し、その入手した復号鍵によって暗号文を解読して捜査に利用する方法が提案されている。この時、供託機関自身の不正を防止するため、１つの供託機関にのみに復号鍵を供託するのではなく、複数の供託機関に分割して供託し、そのうち幾つかの供託機関が協力して、元の復号鍵を復元し、解読に利用する方法である、Micali(S.Micali、“Fair Public-Key Cryptosystems”、Proceedings of Crypto’92、111-138)の方法がある。

【０００４】また、機密データの漏洩を防ぐ手段の１つとして、例えば特開平８－４４６３２公報「ファイル暗号装置」等のファイルを暗号化する方法がこれまでにいくつか提案されている。暗号化したファイルは、そのファイルを暗号化したユーザだけが復号することができる。

【０００５】

【発明が解決しようとする課題】ところが、Shamirの方法では、Ｋ人が集まると、秘密鍵そのものが復元されてしまう。よって、その秘密鍵で復号可能な全てのデータを復号することができ、復号目的以外の必要以上の他の情報がＫ人の人間に知られてしまう危険性がある。

【０００６】一方、Micaliの方法では、組み合わせの数が大きくなると供託機関が持つ分割した復号鍵の数が大きくなるという問題があった。例えば、５つの供託機関があり、このうち３つが協力して鍵を持つとなると、機関Ａは、ＢとＣ、ＢとＤ、ＢとＥ、ＣとＤ、ＣとＥ、ＤとＥ、という具合に協力機関の組み合わせ数だけ分割鍵を持つ必要があり、分割した復号鍵の管理が面倒で複雑化し、そのコストが嵩むという問題があった。

【０００７】また、これらの方法では復号鍵の復元の際に特定の誰かを必須にしたり、分割鍵の所有者をグループ化してそれぞれのグループ内で協力が成立しないと復元できないようにする、といった柔軟な分割が行えなかった。

【０００８】また、分割鍵保有者の変更の場合には、旧保有者の結託による不正な復号鍵の復元を防ぐために秘密鍵を分割し直す必要があるが、全員に再配布しなければならず影響範囲が大きい、という問題も起きてしまう。

【０００９】さらに、特定の復号鍵を復元する際に、特定の誰かを必須にすることは、上記の方法でも必須の分割鍵保有者に複数の分割鍵を割り当てることで実現できていたが、この場合でも分割鍵保有者の変更時には全員に再配布する必要があった。

【００１０】さらに、ファイルを暗号化する場合については、特開平８－４４６３２公報「ファイル暗号装置」等の装置では、暗号化ファイルを所有するユーザしかファイルを復号することができない。このため、企業内で担当者が作成した文書を、前記装置を用いて暗号化した場合、顧客や他部署などから前記文書に関する問い合わせがあったときに、前記担当者が不在の場合には前記文書を復号できないという問題があった。

【００１１】さらに、前記公報に開示された「ファイル暗号装置」では、ファイルを復号する際にパスワードの入力を求められるが、パスワードを忘れてしまうとファイルを復号できないという問題もあった。

【００１２】本発明の目的は、秘密鍵自体を知られること無く、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータあるいはファイルを復号でき、かつその分割鍵の管理も容易であるデータ復号方法を提供することにある。

【００１３】本発明の他の目的は、分割鍵を復元する際に特定の誰かが保有する分割鍵を必須の条件としたり、分割鍵の所有者をグループ化してそれぞれのグループ内で協力が成立しないと復元できないようにするなどの柔軟な分割を行い、その分割された鍵を用いて、暗号化されたデータを復号することができるデータ復号方法を提供することにある。

【００１４】本発明のさらに他の目的は、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータあるいはファイルを簡単な操作で容易に復号することができるデータ復号装置を提供することにある。

【００１５】

【課題を解決するための手段】上記目的を達成するために、本発明は、公開鍵暗号の公開鍵と秘密鍵の鍵ペアのうち秘密鍵をＮ個（Ｎ≧２の整数）に分割し、それぞれの分割鍵をＮ人の分割鍵保有者に割り当てた際の分割鍵保有者の数Ｎに１を加えた数の変数を含む複数の一次式で、かつ１つの変数の係数は常に０でなく、残りＮ個の変数における係数のうちＫ個が０でない複数の一次式を予め記憶した記憶手段を備え、前記Ｎ人のうちＫ（Ｋ＜Ｎ）人に割り当てた分割鍵を用いて前記公開鍵で暗号化されたデータをコンピュータにより復号するデータ復号方法であって、前記秘密鍵を分割する際に、前記記憶手段に記憶された一次式を読み出し、該一次式によって前記秘密鍵をＮ個に分割し、その分割されたＮ個の分割鍵のうちＫ個を用いて前記公開鍵で暗号化したデータを復号することを特徴とする。

【００１６】詳しくは、次に述べるＮ＋１変数の一次式に基づいて秘密鍵を分割して分割鍵保有者に預ける。こ

のうちＫ人が集まれば、暗号化したデータが復号できるように構成し、秘密鍵そのものは復元されないように構成したものである。

【００１７】説明のため、秘密鍵をS’、 S = S’ /2を「１」から「１０」までのある整数とみなし、秘密鍵S’を３人に分割して、２人が集まってデータを復号する場合を例に挙げると、まず、「位数１１」の有限体Z_{11}上で以下の一次式を作成する。

【００１８】

【数１】$1S_1 + 1S_2 + 0_3 = S \pmod{11}$

【００１９】

【数２】$2S_1 + 0S_2 + 1S_3 = S \pmod{11}$

【００２０】

【数３】$0S_1 + 2S_2 + 10S_3 = S \pmod{11}$

ここで、数３は、数１の２倍から数２を引き算することによって得られることに注意する。すると、あるS_1、S_2、S_3、Sについてある２つの式が成立すると、残りの式も成立することになる。公開鍵暗号としては、ある数のべき乗を求めることで復号する方式を選ぶ。

【００２１】また、上記の分割鍵について同様な方法で一次式を作成し、さらに分割を繰り返すことで、分割鍵保有者をグループ化したそれぞれのグループ内での協力と、グループ単位での協力を組み合わせた復号を行うようにする。あるいは、グループ化の際にあるグループでは全員参加の協力とし、さらに全グループでの協力を必要とすることで、ある特定の分割鍵保有者の協力を必須とする条件で復号を行うようにする。

【００２２】また、分割鍵保有者の変更時の課題を解決するため、分割鍵保有者をグループ化したそれぞれのグループ内での協力と、グループ単位での協力を組み合わせた復号を行えるよう、上記方法で秘密鍵を分割した後、分割鍵についても同様に一次式を作成してさらに分割を繰り返すように構成したものである。

【００２３】さらに、本発明のデータ復号方法を適用したデータ復号プログラムをファイル暗号装置に実装し、前記データ復号プログラムのインタフェースを用いてデータあるいはファイルを暗号化する担当者の秘密鍵を分割し、その分割鍵を前記担当者の上長や所属のコンピュータ管理者に保有させ、暗号化操作を行った担当者が不在のときでも、前記データ復号プログラムを用いてコンピュータ管理者等の分割鍵保有者が協力して、暗号化されたデータあるいはファイルを復号できるように構成したものである。

【００２４】

【発明の実施の形態】以下、図面に従い、本発明の実施の形態について説明する。図１は、本発明を適用した暗号データの復号システムの一実施形態を示すシステム構成図である。図１において、１０１は、一般の利用者が使う計算機であり、利用者の作成した文書あるいはファイルを暗号化して保管する。１０２は、鍵生成装置であり、複数の利用者計算機１０１の利用者が使用する暗号の鍵ペア、すなわち公開鍵暗号の公開鍵と秘密鍵を生成する。生成した鍵ペアは利用者計算機１０１に、また秘密鍵は分割して分割鍵保有者計算機１０３に送る。

【００２５】１０３は分割鍵保有者計算機であり、利用者の分割された秘密鍵を保持している。ここでは、Ｎ台の分割鍵保有者計算機１０３が設置されているものと仮定する。

【００２６】１０４はデータ復号装置であり、利用者計算機１０１から復号したい暗号化文書に関する情報を取り出し、Ｋ台（Ｋ＜Ｎ）の分割鍵保有者計算機１０３から部分的に復号された情報を集め、利用者が暗号化した文書を復号する。１０５は、利用者計算機１０１と鍵生成装置１０２とデータ復号装置１０４と分割鍵保有者計算機１０３とを接続するネットワークである。

【００２７】以上の構成において、まず、システム構築時に鍵生成装置１０２において行う処理の概要を図２のフローチャートを参照して説明する。なお、ここで例示するビット数は、本出願時の暗号学により、ある程度の安全性が保証されている数であり、今後大きくなると予想される。また、秘密鍵の分割に必要な計算式等のアルゴリズムは、各計算式を必要とする計算機の内部の記憶装置に予め記憶され、必要の都度読み出されて使用されるものである。

【００２８】まず、ステップ２０１において、暗号パラメータｐ，Ｇを生成する。暗号パラメータｐは、１０２４ビット以上の素数であり、このｐと共に、ｐ＝ 2q＋１なるqも素数になるように求める。そして、ｐを法として位数ｐ－１がとなる数Ｇ（原始根）を求める。定義よりＧは、数４に示すように、ｐを法としてｐ－１乗して始めて「１」となる数である。

【００２９】

【数４】$G_p^{\,p-1} = 1 \pmod{p}$

次に、ステップ２０２において、Ｎ個からＫ個を選択する組み合わせの数${}_NC_K$に等しい個数の恒等式T_iを生成する。生成の方法は図３を用いて後述する。恒等式はZ_qで求める。ここでZ_qは「0」から「q-1」までの整数からなる集合でqを法とした加減乗除の演算を行う。

【００３０】次にステップ２０３において、前記ステップ２０１，２０２において得られたｐ，Ｇを利用者計算機１０１と分割鍵保有者計算機１０３に送り、ｐ，Ｇ，T_iをデータ復号装置１０４に送る。

【００３１】図３は、恒等式T_iの生成方法を示すフローチャートである。なお、ここで分割鍵保有者の数をＮ、復号に必要な分割鍵保有者の数をＫとする。第１例では、Ｎ＝３、Ｋ＝２、ｐ＝２３として、すなわち、３人の分割鍵保有者のうち、２人が協力して復号する場合を例に挙げて具体的に説明する。

【００３２】まず、ステップ３０１、３０２において、変数ｉ，ｊの初期化を行い、ｉ＝１，ｊ＝１とする。

【００３３】次のステップ３０３，３０４，３０５において、恒等式T_iにおけるS_jの係数をランダムに定める。この結果、具体的には、ｉが「１」の時、T_1についてS_1の係数が例えば「５」となる。

【００３４】次のステップ３０６において、S_2とSの係数が「１」、S_3の係数が「０」となる。以上でT_iが決定し、次の、数５の式となる。

【００３５】

【数５】

$$5S_1 + 1S_2 + 0S_3 = S \pmod{11} \quad \cdots T_1$$

次に、ステップ３０７において、ｉが「２」、Ｎが「３」、Ｋが「２」であるので「ｉ≦Ｎ－Ｋ＋１」が成立して、ｉを「２」に更新してステップ３０２、３０３、３０４の処理を同様に行い、T_2のS_jの係数を定める。この結果、具体的には、S_1 の係数が例えば「８」となる。さらにステップ３０６において、S_3 とSの係数が「１」、S_2が「０」となる。以上までで、T_2が定まり、次の、数６のようになる。

【００３６】

【数６】

$$8S_1 + 0S_2 + 1S_3 = S \pmod{11} \quad \cdots T_2$$

次に、ステップ３０８において、S_2とS_3の係数が「０」でないT_3を求めるために、今まで求めた式で、S_2の係数が「０」でない式T_1とS_3の係数が「０」でない式T_2

$$7S_1 + 2S_2 + 1S_3 + 0S_4 + 0S_5 = S \pmod{11} \quad \cdots T_1$$

続くステップ３０７において、ｉが「２」、Ｎが「５」、Ｋが「３」であるので、「ｉ≦Ｎ－Ｋ＋１」が成立して、ｉを「２」に更新してステップ３０２，３０３，３０４の処理を行い、T_2のS_jの係数を定める。例

$$3S_1 + 5S_2 + 0S_3 + 1S_4 + 0S_5 = S \pmod{11} \quad \cdots T_2$$

同様にT_3式が例えば、以下の、数１１のようになる。

【００４４】

$$10S_1 + 3S_2 + 0S_3 + 0S_4 + 1S_5 = S \pmod{11} \quad \cdots T_3$$

以下、同様にしてステップ３０８からステップ３１１で残りの式を求める。

【００４５】５人の分割鍵保有者から３人を選ぶ残りの組み合わせは、（１、３、４）、（１、３、５）、（１、４、５）、（２、３、４）、（２、３、５）、（２、４、５）、（３、４、５）の７つの組み合わせがある。以下、残りの式を先の３つの式から求める。

（１、３、４）に対応するT_4を求めるには、S_3の係数が「０」でないT_1とS_4の係数が「０」でないT_2から計

$$6S_1 + 0S_2 + 9S_3 + 3S_4 + 0S_5 = S \pmod{11} \quad \cdots T_4$$

となる。

【００４８】以下同様にして、T_5、T_6、T_7、T_8、T_9、T_{10}を求めると、以下のようになる。

$$1S_1 + 0S_2 + 3S_3 + 0S_4 + 9S_5 = S \pmod{11} \quad \cdots T_5$$
$$4S_1 + 0S_2 + 0S_3 + 7S_4 + 3S_5 = S \pmod{11} \quad \cdots T_6$$
$$0S_1 + 10S_2 + 2S_3 + 10S_4 + 0S_5 = S \pmod{11} \quad \cdots T_7$$
$$0S_1 + 7S_2 + 7S_3 + 0S_4 + 5S_5 = S \pmod{11} \quad \cdots T_8$$

とを選択する。

【００３７】次に、ステップ３０９において、T_3はS_1の係数が不要、つまり「０」になるようにT_1とT_2から計算する。具体的にはT_1を８倍したものから５倍したT_2を引いてT_3を次の、数７、数８を計算して得る。

【００３８】

【数７】$0S_1 + 8S_2 + 6S_3 = 3S \pmod{11}$

【００３９】

【数８】両辺を３で割って

$$0S_1 + 10S_2 + 2S_3 = S \pmod{11} \quad \cdots T_3$$

以上において法（ｍｏｄ）を「１１」として計算していることに注意する。

【００４０】別の例として、分割鍵保有者が５人で、このうち３人が協力する場合の例を挙げる。この場合、Ｎ＝５、Ｋ＝３となる。

【００４１】まず、ステップ３０３，３０４，３０５において、T_iのS_jの係数を定める。具体的には、iが「１」の時、T_1についてS_1 の係数が例えば「７」、S_2 の係数が例えば「２」となる。さらにステップ３０６においてS_3 とSの係数が「１」、S_4とS_5の係数が「０」となる。T_1は次の、数９の通りとなる。

【００４２】

【数９】

えば、次の、数１０のようにT_2が決まる。

【００４３】

【数１０】

【数１１】

算する。この時、S_2の係数が不要となるので、T_1とT_2でS_2の係数を消去するように計算する。具体的には、５倍のT_1式から２倍のT_2式を引くと以下のT_4が求まる。

【００４６】

【数１２】

$$7S_1 + 0S_2 + 5S_3 + 9S_4 + 0S_5 = 3S \pmod{11}$$

【００４７】

【数１３】両辺を３で割って、

【００４９】

【数１４】

$$0S_1 + 9S_2 + 0S_3 + 3S_4 + 9S_5 = S \pmod{11} \quad \cdots T_9$$
$$0S_1 + 0S_2 + 4S_3 + 6S_4 + 2S_5 = S \pmod{11} \quad \cdots T_{10}$$

最後のT_{10}式は、上の式を用いて計算する。例えば、S_1とS_3とS_4の係数が「０」でないT_4とS_1とS_3とS_5の係数が「０」でないT_5からS_1の係数を消去して得ることができる。

【００５０】ステップ３０９の消去の過程で、必要な係数まで消去される場合がある。ここで必要な係数とはSや上記のT_{10}でいえばS_3、S_4、S_5の係数である。例えば、Nが「３」、Kが「２」の場合で、T_1とT_2式が以下のようになったとする。

【００５１】

【数１５】$1S_1 + 1S_2 + 0S_3 = S \pmod{11}$

【００５２】

【数１６】$1S_1 + 0S_2 + 1S_3 = S \pmod{11}$

S_1を消去するため、数１５から数１６を引くと

【００５３】

【数１７】$0S_1 + 1S_2 + 10S_3 = 0S \pmod{11}$

となり、Sの係数が「０」となり、必要な係数が消えている。このような場合は、最初からやり直す。

【００５４】次に、図４を用いて鍵生成装置１０２にて行う利用者の登録方法を説明する。図４において、先ずステップ４０１において、秘密鍵S’ を「１」以上「p-1」未満の偶数、ここでの例の場合「１」から「２２」の数からランダムに選ぶ。ここでは「１２」と仮定する。さらにＳを秘密鍵Ｓ’ の半分の「６」とする。

【００５５】次にステップ４０２において、秘密鍵Ｓを分割してS_jを求める。ここでは先に求めた一次式を利用して分割秘密鍵S_jを計算する。この分割秘密鍵S_jを計算するための一次式は、鍵生成装置１０２の記憶装置に予め記憶されているものである。

【００５６】

【数１８】$5S_1 + 1S_2 + 0S_3 = S \pmod{11}$

【００５７】

【数１９】$8S_1 + 0S_2 + 1S_3 = S \pmod{11}$

【００５８】

【数２０】$0S_1 + 10S_2 + 2S_3 = S \pmod{11}$

S_1をランダムに定める。すると、数１８よりS_2が、数１９よりS_3が求まる。例えば、$S_1 = 3$とすると、$S_2 = 2$、$S_3 = 4$と分割できる。これは数２０を満たしている。

【００５９】次にステップ４０３において、このS_1、S_2、S_3をそれぞれの分割鍵保有者計算機１０３に分割秘密鍵の内容が他に分からないように送る。送る方法には幾つかあるが、本発明の範囲外であるのでその説明は省略する。

【００６０】次に、ステップ４０４において、秘密鍵S’ と公開鍵Ｙを利用者計算機１０１に登録する。この場合の公開鍵Ｙは、数２１で表される。

【００６１】

【数２１】

$$Y = G^{S'} \pmod{23}$$

【００６２】次に、登録の終わった利用者が計算機１０１を用いて、自分が作成した文書を暗号化する方法について図５のフローチャートを用いて説明する。まず、ステップ５０１において、乱数ＲとＭを生成する。次に、ステップ５０２において、数２２を計算する。

【００６３】

【数２２】

$$C_1 = G^R,$$
$$C_2 = M Y^R$$

【００６４】ここでＹは、ステップ４０４で登録した利用者の公開鍵であり、計算はｐを法として、ここでは「２３」で計算する。

【００６５】次のステップ５０３において、Ｍを秘密鍵暗号の鍵とみなして文書を暗号化する。見なしかたは本発明の範囲外であるので省略する。また、暗号方法には、公開鍵暗号に比べて高速な秘密鍵暗号を用いる。この暗号方法についても本発明の対象外であるので、省略する。続くステップ５０４において、C_1、C_2、Ｍで暗号化した文書を保管する。

【００６６】次に、利用者計算機１０１を用いて暗号化された文書を復号する手順を図６のフローチャートにより説明する。復号する場合、まず、ステップ６０１において、数２３を計算して、Ｍを求める。

【００６７】

【数２３】

$$M = C_2 / (C_1)^{S'} \pmod{23}$$

【００６８】次のステップ６０２において、このＭを秘密鍵暗号の鍵とみなして暗号化した文書を復号する。

【００６９】次に、暗号化した文書をデータ復号装置１０４にて復号する手順を図７のフローチャートを用いて説明する。まず、ステップ７０１において、復号したい文書と対応するC_1とC_2とを利用者計算機１０１から取り出す。

【００７０】次に、ステップ７０２において、Ｋ個の利用する分割鍵保有者計算機１０３を選択し、その計算機１０３との安全な通信路を確立する。選択と安全な通信路の確立に付いては、本発明の範囲外であるので省略する。

【００７１】次にステップ７０３において、上記通信路を使って、C_1を分割鍵保有者計算機１０３に送る。そして、ステップ７０４において、各分割鍵保有者計算機１０３が計算した部分復号結果D_jを受け取る。このD_jは、数２４で表される。

【００７２】
【数２４】

【数２４】

$$D_i = C_2^{S_i} \pmod{23}$$

【００７３】次に、ステップ７０５において、数２５を計算し、平文Mを得る。
【００７４】
【数２５】

【数２５】

$$M = C_1 / \prod D_i^{2^{T_{ij}}}$$

【００７５】ここでT_{ij}はどの分割鍵保有者計算機１０３を選んだかによって決まる。先の恒等式を用いて、具体的に説明すると、選んだ分割鍵保有者計算機１０３に対応する係数が「０」でない式を選び、その式のS_jの係数をT_{ij}とする。例えば、２番目と３番目の分割鍵保有者計算機１０３を選んだとすると、次の、数２６を選択する。
【００７６】
【数２６】$0S_1 + 10S_2 + 2S_3 = S \pmod{11}$
すると、$T_{31} = 0$、$T_{32} = 10$、$T_{33} = 2$となる。すると、数２７を計算することで、Mが得られる。
【００７７】
【数２７】

【数２７】

$$C_2 / (D_2^{2^{T_{32}}} \times D_3^{2^{T_{33}}}) = M Y^R / D_2^{20} D_3^4 = M Y^R / C_1^{20S_2} C_1^{4S_3}$$
$$= M G^{2SR} / C_1^{20S_2+4S_3} = M G^{2SR} / C_1^{2S} = M G^{2SR} / G^{2RS} = M$$

【００７８】次に、ステップ７０６において、Mを使って、暗号化した文書を復号する。図８は、以上の処理全体を分かり易くまとめたものであり、利用者計算機１０１の記憶手段１０６に格納された「価格表」と「在庫表」の暗号文書をデータ復号装置１０４で復号する例を示している。なお、図中のパラメータは上記の説明と同じである。また、共通パラメータＧ，ｐは、各計算機の記憶手段１０７に記憶されるようになっている。また、秘密鍵の分割式は鍵生成装置１０２の記憶手段１０８に予め記憶されるようになっている。
【００７９】上記説明では、複数の分割鍵保有者計算機１０３に分割秘密鍵を保有させる例を説明したが、本発明は複数の鍵供託機関に供託しておく場合に同様に適用することができる。以下、図９を用いて、本発明を鍵供託に用いた場合を簡単に説明する。
【００８０】図９において、１１０は受信者計算機、１１１は送信者計算機、１１２－１～１１２－Ｎは複数の供託機関計算機、１１３は鍵生成装置、１１４は公開鍵配布機関計算機、１１５は捜査機関における計算機である。
【００８１】ユーザ登録の際は、鍵を生成した後、公開鍵Ｙは公開鍵配布機関計算機１１４に送信し、秘密鍵Ｓ’は利用者に送る。
【００８２】暗号文を送りたい送信者計算機１１１の送信者は、受信者計算機１１０の受信者の公開鍵Ｙを公開鍵配布機関計算機１１４から入手し、先の例と同じ方法で暗号化して、C_1とC_2と暗号化した文書を受信者計算機１１０に送る。受信者計算機１１０の受信者は、先の例と同じようにして文書を復号する。
【００８３】犯罪の疑いがある場合は、捜査機関の計算機１１５の担当者は送信者計算機１１１から受信者計算機１１０への通信文を盗聴して、C_1とC_2と暗号化した文書を入手する。解読の手順は回復の手順と同じである。
【００８４】以上のように、本実施形態によれば、暗号文を復号する際には秘密鍵そのものはどこにも復元されず、分割鍵保有者計算機１０３が持つ分割鍵S_iに基づいて部分的に復号したデータD_iを使って必要な文書を復号しているため、同じ鍵を用いて、暗号化した他の文書を復号することはできない。
【００８５】また、秘密鍵自体を知られることもない。そして、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータを目的とする暗号文のみに限って復号することができ、かつその分割鍵の管理も容易である。
【００８６】次に、本発明の第２の実施形態について説明する。この第２の実施形態は、Ｎ人の分割鍵保有者をN_G個の複数のグループに分け、そのうちのK_G個（$K_G < N_G$）のグループにおいて、それらのグループに所属するN_g人（$N_g \geq 2$の整数）うちK_g人（$K_g < N_g$）が協力してデータを復号する場合の方法に関するものである。なお、システム構成は図１と同じであり、以下では、図１のシステム構成を前提にして本実施形態における秘密鍵のグループ分割方法と、分割鍵によるデータの復号方法について説明する。
【００８７】まず、本実施形態における秘密鍵のグループ分割方法において、システム構築時において鍵生成装置１０２で行う処理の概要について図１０のフローチャートを参照して説明する。
【００８８】まず、ステップ１００１において、図２のステップ２０１と同様にして暗号パラメータp，q，Ｇを求める。
【００８９】次に、ステップ１００２において、図２のステップ２０２と同様にして、N_G個からK_G個を選択する組み合わせの数$_{NG}C_{KG}$に等しい個数の一次式T_aを生成する(a=1, 2, …, $_{NG}C_{KG}$)。また、ステップ２０２と同様にしてN_g個からK_g個を選択する組み合わせの数に等しい個数の一次式T_{gi}を生成する(g=1, 2, …, N_g)。これは、図３と同様の手順で生成するが、詳細は図１１にて説明す

る。

【００９０】次にステップ１００３において、図２のステップ２０３と同様に、前記ステップ１００１，１００２において得られた暗号パラメータｐ，ｑ，Ｇを利用者計算機１０１と分割鍵保有者計算機１０３に送り、ｐ，Ｇ，T_a、T_{gii}をデータ復号装置１０４に送る。

【００９１】図１１は、恒等式T_a、T_{gi}の生成方法を示すフローチャートである。なお、ここでは、Ｎ＝４、N_G＝２、K_G＝２、N_1＝１、K_1＝１、N_2＝３、K_2＝２、ｐ＝２３とする。

【００９２】これは、Ａ、Ｂ、Ｃ、Ｄの４人のうち３人が協力し、かつＡが必須となるように秘密鍵を分割するのに相当するグループ分けである。すなわち、図１４（ａ）に示すように、グループ１のメンバーはＡのみ、グループ２のメンバーはＢ、Ｃ、Ｄの３人といったグループ分けである。

【００９３】まず、ステップ１１０１において、N_Gが２、K_Gが２の場合における恒等式T_aの変数S_gの係数を定める。その方法は図３と同じである。ここでは、例えば次のような恒等式T_1が得られたとする。

【００９４】

【数２８】$2S_1 + S_2 = S \pmod{11}$

次に、ステップ１１０２において、変数gの初期化を行い、g＝１とする。次に、ステップ１１０３において、N_1個からK_1個を選択する組み合わせの数に等しい個数の一次式T_{1i}を生成する。ここではN_1が１、K_1が１であるため、例えば次のような恒等式T_{1i}が得られたとする。

【００９５】

【数２９】$3S_{11} = S_1 \pmod{11}$

次に、ステップ１１０４において、g=g＋１に更新した後、次のステップ１１０５でg≦ N_Gかを判定する。ここでは、gが２であるので、ステップ１１０３に戻る。ステップ１１０３では、N_2個からK_2個を選択する組み合わせの数に等しい個数の一次式T_{2i}を生成する。ここではN_2＝３、K_2＝２であるため、例えば次のような恒等式T_{2i}が得られる。

【００９６】

【数３０】$5S_{21} + 1S_{22} + 0S_{23} = S_2 \pmod{11}$

$8S_{21} + 0S_{22} + 1S_{23} = S_2 \pmod{11}$

$0S_{21} + 10S_{22} + 2S_{23} = S_2 \pmod{11}$

続くステップ１１０４、１１０５の処理を行うことにより、g=3となり、図１１の処理を終える。

【００９７】次に、図１２を用いて、鍵生成装置１０２にて行う利用者の登録方法を説明する。まず、ステップ１２０１において、図４のステップ４０１と同様に、秘密鍵S’とその半分の値Sを求める。次に、ステップ１２０２において、T_aを使ってSを分割しS_gを求める。この場合の求め方は、図４のステップ４０２と同様に、S_1をランダムに定めてからS_2を計算する。ここで得られたS_1はグループ１に、S_2はグループ２に割り当てるものとする。

【００９８】次にステップ１２０３において、ｇ＝１に設定し、次のステップ１２０４においてT_{gi}に合わせて各S_gを分割しS_{gj}を求める。求め方は図４のステップ４０２と同様である。続いて、g≦ N_Gかを判定し、ＹＥＳならばステップ１２０３に戻って同様の処理を繰り返し、T_{gi}に合わせて各S_gを分割しS_{gj}を求める。次に、ステップ１２０７において、分割した鍵S_{gj}を分割鍵利用者計算機１０３_{gj}に秘密裏に送って登録する。

【００９９】ここでは、図１４（ａ）示すように、S_{11}を分割鍵保有者Ａが利用する分割鍵保有計算機１０３_{11}に、S_{21}、S_{22}、S_{23}を分割鍵保有者Ｂ、Ｃ、Ｄが利用する分割鍵保有計算機１０３_{21}、１０３_{22}、１０３_{23}に配布して登録する。

【０１００】最後に、ステップ１２０８において、図４のステップ４０４と同様に、秘密鍵S’と公開鍵$Y=G_{S'}$を利用者計算機１０１に送る。

【０１０１】利用者計算機１０１では、鍵生成装置１０２から配付された秘密鍵S’と公開鍵$Y=G_{S'}$を用いて文書やファイルの暗号化、および復号を行う。

【０１０２】次に、図１３のフローチャートを用いて、暗号化した文書を、各分割鍵保有者が利用する各分割鍵保有計算機１０３_{11}、１０３_{21}、１０３_{22}、１０３_{23}との協同作業によってデータ復号装置１０４にて復号する手順について説明する。

【０１０３】まず、ステップ１３０１において図７のステップ７０１と同様に、復号したい文書と対応するC_1とC_2とを利用者計算機１０１から取り出す。

【０１０４】次に、ステップ１３０２において、N_G個のグループ中から選んだK_G個の各グループについて、K_g個の分割鍵保有者計算機１０３を選択し、図７のステップ７０２と同様にその計算機との安全な通信路を確立する。

【０１０５】ここではグループ１の分割鍵保有者Ａが使用する分割鍵保有計算機１０３_{11}、グループ２の分割鍵保有者Ｃ、Ｄが使用する分割鍵保有計算機１０３_{22}、１０３_{23}を選んだものとする。

【０１０６】次に、ステップ１３０３において、図７のステップ７０３と同様に、上記通信路を使ってC_1を分割鍵保有者計算機１０３_{11}、１０３_{22}、１０３_{23}に送る。

【０１０７】次に、ステップ１３０４において図７のステップ７０４と同様に、これらの分割鍵保有者計算機上で計算した部分解読結果D_{gj}を受け取る。この部分解読結果D_{gj}は、次の、数３１で表される。

【０１０８】

【数３１】

【数３１】

$$D_{gj} = C_1^{2Sgj} \pmod{23}$$

【０１０９】次に、ステップ１３０５において図７のス

テップ７０５と同様な計算を行うことにより、平文Mを得る。この平文Mは、次の、数３２で表される。

【０１１０】

【数３２】

【数３２】

$$M = C_2 / \Pi_{ij} D_{ij}^{2 t_{ag} t_{gij}}$$

【０１１１】ここで、t_{ag}は、どのグループを選んだかによって決まる。恒等式T_aから、選んだグループに対応する係数が０でない式を選び、その式のS_gの係数をt_{ag}とする。ここではT_aは次の、数３３に示すT_1ただ１つしかなく、t_{11}は２、t_{12}は１となる。

【０１１２】

【数３３】$2S_1 + S_2 = S \pmod{11}$

また、t_{gij}はどの分割鍵保有者計算機１０３$_{gi}$を選んだかによって決まる。各グループについて、そのグループに対応する恒等式T_{gi}から、選んだ分割鍵保有者計算機１０３に対応する係数が０でない式を選び、その式のS_{gj}の係数をt_{gij}とする。ここでは、１つ目のグループについては次の、数３４に示す恒等式T_{11}

【０１１３】

【数３４】$3S_{11} = S_1 \pmod{11}$

から、t_{111}＝３となる。２つ目のグループについては、例えば２番目と３番目の計算機１０３$_{22}$、１０３$_{23}$を選んだとすると、次の、数３５に示す恒等式T_{23}

【０１１４】

【数３５】$0S_{21} + 10S_{22} + 2S_{23} = S_2 \pmod{11}$

から、t_{232}＝１０、t_{233}＝２となる。すると、

【０１１５】

【数３６】

【数３６】

$$\begin{aligned} & C_2 / (D_{11}^{2 t_{111}} \times D_{22}^{2 t_{122} t_{232}} \times D_{23}^{2 t_{123} t_{233}}) \\ & = MY_F / D_{11}^{12} D_{22}^{20} D_{23}^{4} = MY^R / C_1^{12 S_{11}} C_1^{20 S_{22}} C_1^{4 S_{23}} \\ & = MG^{2SR} / C_1^{2\{2(3S_{11}) + 1(10S_{22} + 2S_{23})\}} = MG^{2SR} / C_1^{2(2S_1 + S_2)} \\ & = MG^{2SR} / C_1^{2S} = MG^{2SR} / G^{2RS} = M \end{aligned}$$

【０１１６】を計算することで、平文Mが得られる。このようにして平文Mが得られたならば、ステップ１３０６において、Mを使って暗号化した文書を復号する。

【０１１７】以上のように秘密鍵を分割することにより、暗号文の復号に際しては、ユーザＡの協力が必須となる復号形態を実現することができる。

【０１１８】なお、図１４（ａ）において、「２／２に分割」、「１／１に分割」、「２／３に分割」とは、分割数と必須となる分割鍵の数を表すものであり、分母が分割数、分子が必須となる分割鍵の数を示している。図１４（ａ）のような分割を行った場合に、S_{11}の保有者が変わったとしても、S_1を図３の方法を使ってS'_{11}を生成し、新たな保有者に配ればよい。同様にS_{21}、S_{22}、S_{23}のいずれかの保有者が変わっても、S_2を分割し直してそのグループ内で配布し直せばよい。あるいはグループ内でS_2を分割する条件を変えてもその影響範囲はそのグループ内に限ることができる。

【０１１９】なお、本発明は図１４（ａ）に示すような分割の仕方に限らず、同図（ｂ）に示すような様々な分割の仕方をすることができる。

【０１２０】次に、本発明の第３の実施形態について説明する。この第３の実施形態は、１つの利用者計算機内で上述した方法によって秘密鍵を複数に分割し、各分割鍵を別々の利用者に割り当てておき、暗号文を復号する際に分割鍵の保有者の全部または必須とされる分割鍵の保有者の協力により、暗号文を復号するようにしたものであり、特に、復号する際のインタフェースの構成に関するものである。

【０１２１】図１５は、第３の実施形態のシステム構成を示す図であり、１５００は一般の利用者が使う計算機（利用者計算機）であり、中央処理部１５０１、入出力部１５０２、表示部１５０３、ファイル暗号部１５０４、鍵生成部１５０５、ファイル復号部１５０６から構成される。この利用者計算機１５００は、例えばパーソナルコンピュータ等の汎用の計算機で構成することができる。

【０１２２】中央処理部１５０１は、システム構築、恒等式の作成、ユーザ登録、ファイル暗号、ファイル復号、入出力、表示などの一連の処理を制御する。

【０１２３】入出力部１５０２は、復号したいファイルあるいはデータの名前を入力したり、分割鍵を入出力したりするためのものである。この入出力部１５０２には、キーボード、マウス、フロッピーディスクドライブなどが用いられる。

【０１２４】表示部１５０３は、ファイル復号などの案内画面を表示するためのものである。この表示部１５０３には、ディスプレイなどが用いられる。

【０１２５】ファイル暗号部１５０４は、利用者の作成した文書を暗号化して図示しない記憶装置に保管する部分であり、図１の利用者計算機１０１と同様の機能を有する。

【０１２６】鍵生成部１５０５は、図１の鍵生成装置１０２と同様の機能を有するものであり、利用者が使用する暗号の鍵ペア、すなわち公開鍵暗号の公開鍵と秘密鍵を生成する。生成した鍵ペアはファイル暗号部１５０４に、また秘密鍵は分割して入出力部１５０２に送る。

【０１２７】ファイル復号部１４０６は、図１のデータ復号装置１０４と同様の機能を有するものであり、ファ

イル暗号部１５０４から復号したい暗号化ファイルに関する情報を取り出し、K個の分割鍵を集め、いずれかの利用者が暗号化したファイルを復号する。

【０１２８】前述の第１の実施例では、システムを構成する各装置がネットワーク１０５で接続されているが、本実施形態では、システムを構成する各部はすべて利用者計算機１５００内にあり、ファイル復号に関する一連の処理はすべて利用者計算機１５００内で行われる。

【０１２９】図１６のフローチャートを用いて、システム構築時に行う処理の概要を説明する。まず、ステップ１６０１において、図２のステップ２０１と同様にして暗号パラメータp、q、Gを求める。次に、ステップ１６０２において、図２のステップ２０２と同様にして恒等式T_iを生成する。生成の方法は図３と同様である。

【０１３０】続く、ステップ１６０３において、暗号パラメータp、Gをファイル暗号部１５０４に、p、G、T_iをファイル復号部１５０６に送る。

【０１３１】図１７は、鍵生成部１５０６にて行う利用者の登録方法を示すフローチャートである。まず、ステップ１７０１において、図４のステップ４０１と同様にしてSを選ぶ。次に、ステップ１７０２において、図４のステップ４０２と同様にして分割鍵S_jを求める。次に、ステップ１７０３において、各S_jに対して、分割鍵保有者認証情報I_jを付加する。I_jは、分割鍵保有者のID、パスワードなどの情報から構成されており、中央処理部１５０１が管理する。

【０１３２】次に、ステップ１７０４において、分割した鍵S_jを入出力部１５０２に出力し、認証情報I_jを表示部１５０３に表示する。出力された分割鍵S_jは、フロッピーディスクやＩＣカード等の携帯可能な記録媒体に格納し、各分割鍵保有者が安全な場所に保管する。表示された認証情報I_jは、各分割鍵保有者が他人に漏らさないように記憶しておくようにする。

【０１３３】次に、ステップ１７０５において、図４のステップ４０４と同様にして秘密鍵2S とYをファイル暗号部１５０４に登録する。

【０１３４】なお、本実施形態では、分割鍵S_jを各分割鍵保有者が安全に管理することを要求しているが、分割鍵S_jが入ったフロッピーディスク等の記録媒体の盗難などに対応するために、分割鍵S_jを記録媒体に格納する際に、パスワードで暗号化しておいて、図１８で説明する分割鍵保有者認証の際に分割鍵S_jを復号するようにしてもよい。

【０１３５】次に、図１８を用いて、複数の分割鍵保有者が協力して、利用者が暗号化したファイルを復号する手順を示す。なお、利用者がファイルを暗号化する方法と、利用者自身が暗号化されたファイルを復号する手順は、それぞれ図５、図６と同様である。

【０１３６】まず最初に、ファイル復号に必要な人数の分割鍵保有者に、各自の分割鍵が格納された記録媒体を持って集合してもらう。この状態で、ステップ１８０１において、分割鍵保有者の代表者または利用者計算機１５００の管理者が、ファイル復号部１５０６を起動する。このファイル復号部１５０６やファイル暗号部１５０４および鍵生成部１５０５は、具体的には、ファイル復号プログラム、ファイル暗号プログラム、鍵生成部プログラムによって構成されるものである。

【０１３７】ファイル復号部１５０４が起動すると、中央処理部１５０１はステップ１８０２において、表示部１５０３にファイル復号情報を表示する。図１９は、ファイル復号情報の画面表示例であり、分割鍵保有者の登録人数「３」と、ファイル復号に必要な分割鍵保有者の人数「２」が表示されている。

【０１３８】ファイル復号情報が表示されると、１人目の分割鍵保有者は、図１９中の「ＯＫ」ボタンをクリックする。１人目の分割鍵保有者が「ＯＫ」ボタンをクリックすると、中央処理部１５０１は、ステップ１８０３において、表示部１５０３に分割鍵保有者認証画面を表示する。図２０は、分割鍵保有者認証画面の表示例である。なお、ステップ１８０３において、分割鍵保有者が図２０中の「キャンセル」ボタンをクリックした場合は、ファイル復号処理が中止される。本実施形態では、「キャンセル」ボタンが表示されている画面で、分割鍵保有者が「キャンセル」ボタンをクリックすると、ファイル復号処理を中止することができる。

【０１３９】分割鍵保有者認証画面が表示されると、ステップ１８０４において、分割鍵保有者は、分割鍵S_jが格納された記録媒体を挿入し、ＩＤ、パスワードからなる認証情報を入力した後、図２０中の「ＯＫ」ボタンをクリックする。

【０１４０】「ＯＫ」ボタンがクリックされると、中央処理部１５０１は、入力された認証情報と自身が管理している認証情報I$と_j$を照合し、１人目の分割鍵保有者の認証を行う。なお、本実施形態では、分割鍵保有者の認証にパスワードを用いているが、分割鍵保有者の認証には、例えば指紋などによる他の認証方法を用いてもよい。

【０１４１】次に、中央処理部１５０１は、ステップ１７０５において、分割鍵保有者の必要な人数分の認証を行ったかどうかをチェックする。必要人数に達していない場合は、ステップ１８０３に戻って、分割鍵S_jの入力および分割鍵保有者の認証を繰り返す。

【０１４２】必要人数に達した場合は、中央処理部１５０１は、ステップ１８０６において、表示部１５０３にファイル・保存先入力画面を表示する。図２１は、ファイル・保存先入力画面の表示例である。

【０１４３】ファイル・保存先入力画面が表示されると、分割鍵保有者は、復号したいファイルの名前を入力するか、または図２１中の上段の「参照」ボタン２１０１をクリックし、復号したいファイルの場所を参照す

る。

【０１４４】分割鍵保有者が「参照」ボタン２１０１をクリックすると、ステップ１８０７において、中央処理部１５０１は、表示部１５０３にファイル参照画面を表示する。図２２は、ファイル参照画面の表示例である。

【０１４５】ファイル参照画面が表示されると、分割鍵保有者は、前記ファイル参照画面から復号したいファイルを選択する。例えば「ｒｅａｄｍｅ．ｔｘｔ」を選択する。

【０１４６】ステップ１８０６で分割鍵保有者がファイルの名前を入力するか、またはステップ１８０７で分割鍵保有者がファイルを選択すると、ステップ１８０８において、中央処理部１５０１は、表示部１５０３にファイル・保存先入力画面を再び表示する。図２３は、ファイル・保存先入力画面の表示例である。復号したいファイルの名前と、ファイル復号後の保存先が表示されている。

【０１４７】ファイル・保存先入力画面が表示されると、ステップ１８０９において、分割鍵保有者は、保存先を変更するかどうかを指定する。保存先を変更する場合は、分割鍵保有者は、保存先を直接入力するか、または図２３中の下段の「参照」ボタン２３０１をクリックする。保存先を変更しない場合は、ステップ１８１１へ進む。

【０１４８】ステップ１８０９で分割鍵保有者が「参照」ボタン２３０１をクリックすると、ステップ１８１０において、中央処理部１５０１は、表示部１５０３に保存先参照画面を表示する。図２４は、保存先参照画面の表示例である。

【０１４９】保存先参照画面が表示されると、分割鍵保有者は、前記保存先参照画面からファイル復号後の保存先を入力する。保存先が入力されると、中央処理部１５０１は、表示部１５０３にファイル・保存先入力画面を再び表示する。保存先が決まると、ステップ１８１１において、分割鍵保有者は、図２３中の「回復」ボタンをクリックする。

【０１５０】分割鍵保有者が「回復」ボタンをクリックすると、中央処理部１５０１は、ファイル復号部１５０６に対して、入力されたファイルの復号処理を依頼する。ファイルが復号されると、中央処理部１５０１は、入力された保存先に復号されたファイルを保存する。ファイル復号処理の詳細は図２６で説明する。

【０１５１】ファイルが保存されると、ステップ１８１２において、中央処理部１５０１は、表示部１５０３に終了画面を表示する。図２５は、終了画面の表示例である。復号したファイルの所有者「ｒｙｏｋｏ」と名前「Ｃ：￥ｔｅｍｐ￥暗号ｒｅａｄｍｅ．ｔｘｔ」が表示されている。終了画面が表示されると、分割鍵保有者は、図２５中の「ＯＫ」ボタンをクリックしてファイル復号処理を終了する。

【０１５２】本発明の実施形態には、以上に説明したものの他に様々なバリエーションが考えられる。以下、図１８のファイル復号フロー図のステップの変更という形で、前記バリエーションについて説明する。

【０１５３】まず、ステップ１８０３～１８０５の分割鍵保有者認証と、１８０６～１８１０のファイル・保存先入力の手順とは、互いに入れ換えることが可能である。また、ステップ１８１１でファイルを復号した後、図２５の終了画面の代わりにファイルオープン選択画面を表示して、分割鍵保有者がファイルオープンを選択した場合には、前記ファイルに関連付けられたアプリケーションプログラムを起動して、前記アプリケーションから復号したファイルを開くようにしてもよい。

【０１５４】図２７は、ファイルオープン選択画面の表示例である。復号したファイルの所有者と名前が表示されている。

【０１５５】分割鍵保有者は、復号したファイルを開く場合は図２７中の「はい」ボタンを、開かない場合は図２７中の「いいえ」ボタンをクリックする。分割鍵保有者が「はい」ボタンをクリックした場合は、ファイルを関連アプリケーションで開く。図２７に示した例では、復号したファイルはテキストファイルであるので、この場合は通常テキストエディタが起動して前記ファイルが開くことになる。

【０１５６】本実施形態では、復号するファイルの数は１個だけであったが、ステップ１８０６において、分割鍵保有者がファイルを複数入力できるようにして、複数のファイルを復号できるようにしてもよい。この場合、各ファイルの復号後の保存先のディレクトリを同じにしてもよいし、ファイルごとに別々にしてもよい。

【０１５７】また、前記ファイルの複数入力をさらに発展させて、ステップ１８０６で分割鍵保有者がディレクトリを指定できるようにして、前記ディレクトリに属するすべてのファイルを一度に復号できるようにしてもよい。

【０１５８】本実施形態では、ファイル復号部（ファイル復号プログラム）１５０６を起動してから復号するファイルを選択していたが、例えばファイラーから予め復号したいファイルを選んでおき、マウスの右ボタンをクリックするなどの方法でポップアップメニューを表示し、前記ポップアップメニューからファイル復号部１５０６を起動するといった方法もある。

【０１５９】分割鍵保有者がファイルの内容を確認したいだけならば、復号したファイルを必ずしもどこかに保存する必要はない。復号したファイルをテンポラリファイルとしておき、関連アプリケーション起動後に前記テンポラリファイルを開き、前記アプリケーションを終了すると前記テンポラリファイルが消去されるようにしてもよい。

【０１６０】ファイル復号部１５０６を、復号したいフ

ファイルがある利用者計算機から起動する必要もない。復号したいファイルがある利用者計算機から、前記ファイルのC_1、C_2などのファイル復号に必要な情報を取り出して、フロッピーディスクなどの持ち運び可能な媒体に格納し、分割鍵保有者の計算機などの他の計算機からファイル復号部１５０６を起動して、前記媒体内の情報からファイルを復号させてもよい。以上に説明したバリエーションを複数組み合わせるといったことも可能である。

【０１６１】図２６を用いて、暗号化したファイルをファイル復号部１５０６にて復号する手順について説明する。まず、ステップ２６０１において、図７のステップ７０１と同様にして、復号したい文書と対応するC_1とC_2とをファイル暗号部１５０４から取り出す。次に、ステップ２６０２において、各S_jを中央処理部１５０１から取り出す。続くステップ２６０３において、各D_jを次の、数３７によって計算する。

【０１６２】

【数３７】

【数３７】

$$D_j = C_1^{Sj}$$

【０１６３】本実施形態では、ファイル復号処理はすべて同一の利用者計算機上で行っている。このため、ステップ２６０２、２６０３では、図７と異なり、各S_jからD_jを直接計算している。

【０１６４】次に、ステップ２６０４において、図７のステップ７０５と同様にして平文Mを求める。

【０１６５】

【数３８】

【数３８】

$$M = C_2 / \Pi D_j^{2Tij}$$

【０１６６】次に、ステップ２６０５において、平文Mを使って、暗号化した文書を復号する。なお、上記各実施形態において、各計算機が実行する処理は、ＣＤ－ＲＯＭ等の記録媒体に記録して各計算機にインストールして実行するように構成することができる。あるいは、記録媒体に代えて、インターネット等の通信媒体を用いて各計算機にインストールして実行させることができる。

【０１６７】また、本発明の適用範囲である鍵の分割は個人単位に限定されるものではなく、団体、グループを対象としても構わない。

【０１６８】

【発明の効果】以上の説明から明らかなように、本発明によれば、暗号文を復号する際には秘密鍵そのものはどこにも復元されず、分割鍵保有者計算機が持つ分割鍵S_iに基づいて部分的に復号したデータD_iを使って必要な文書を復号しているため、同じ鍵を用いて、暗号化した他の文書を復号することはできない。

【０１６９】また、秘密鍵自体を知られることもない。そして、複数人の分割鍵保有者の協力により、公開鍵で暗号化されたデータを目的とする暗号文のみに限って復号することができ、かつその分割鍵の管理も容易である。

【０１７０】供託機関に供託した鍵を用いるようにした場合、１人のユーザに対して１つの分割鍵を持っており、従来技術としてあげたMicaliの方法のように１人に対して複数の分割鍵を保管する必要がないので、保管のコストを下げることができる。

【０１７１】したがって、例えば、企業内で担当者が作成、暗号化した文書を、その担当者がいない時に復号する必要が生じた場合、担当者の上長や所属のコンピュータ管理者が協力して復号する場合に好適である。

【０１７２】また、公開鍵暗号の秘密鍵供託方式において、特に複数の供託機関に秘密鍵を分割して供託する場合にも好適である。

【０１７３】さらに、分割鍵保有者をグループ化することにより、復号の際には上位の権限を持つ分割鍵保有者の参加を必ず必要とする運用が可能となる。

【０１７４】さらに、分割鍵保有者をグループ化することにより、保有者変更時の分割鍵再配布の範囲を狭くしたり、復号の際には上位の権限を持つ分割鍵保有者の参加を必ず必要としたりする、柔軟な運用が可能となる。

【０１７５】さらに、本発明のデータ復号インタフェースを用いれば、分割鍵保有者が暗号ファイルを容易に復号することができるので、担当者不在時の問い合わせにも、前記担当者所有の暗号ファイルを復号して内容を確認することで対応できる。また、前記担当者がパスワードを忘れた場合にも対応できる。

【図面の簡単な説明】

【図１】本発明を適用した暗号データの復号システムの一実施形態を示すシステム構成図である。

【図２】システム構築時に行う処理の概要示すフローチャートである。

【図３】恒等式T_iの生成方法を示すフローチャートである。

【図４】鍵生成装置にて行う利用者の登録方法を示すフローチャートである。

【図５】利用者計算機を用いて、自分が作成した文書を暗号化する手順を示すフローチャートである。

【図６】利用者計算機を用いて暗号化された文書を復号する手順を示すフローチャートである。

【図７】暗号化した文書をデータ復号装置にて復号する手順を示すフローチャートである。

【図８】図７までの処理全体を分かり易くまとめた説明図である。

【図９】本発明を鍵供託に用いた場合の復号方法の説明図である。

【図１０】本発明の第２の実施形態において、システム構築時に行う処理の概要を示すフローチャートである。

【図１１】第２の実施形態における恒等式T_iの生成方

法を示すフローチャートである。

【図１２】第２の実施形態における鍵生成装置にて行う利用者の登録方法を示すフローチャートである。

【図１３】第２の実施形態における利用者計算機を用いて、自分が作成した文書を暗号化する手順を示すフローチャートである。

【図１４】秘密鍵のグループ分割の仕方の例を示す図である。

【図１５】本発明の第３の実施形態を示すシステム構成図である。

【図１６】第３の実施形態において、システム構築時に行う処理の概要を示すフローチャートである。

【図１７】第３の実施形態における利用者の登録方法を示すフローチャートである。

【図１８】第３の実施形態において、利用者計算機を用いて暗号化された文書を分割鍵保有者の鍵を用いて復号する手順を示すフローチャートである。

【図１９】第３の実施形態において表示部に表示されるファイル回復情報画面の例を示す図である。

【図２０】第３の実施形態において表示部に表示される管理者認証画面の例を示す図である。

【図２１】第３の実施形態において表示部に表示されるファイル・保存先入力画面の例を示す図である。

【図２２】第３の実施形態において表示部に表示されるファイル参照画面の例を示す図である。

【図２３】第３の実施形態において表示部に表示されるファイル・保存先入力画面の例を示す図である。

【図２４】第３の実施形態において表示部に表示される保存先参照画面の例を示す図である。

【図２５】第３の実施形態において表示部に表示されるデータ復号終了画面の例を示す図である。

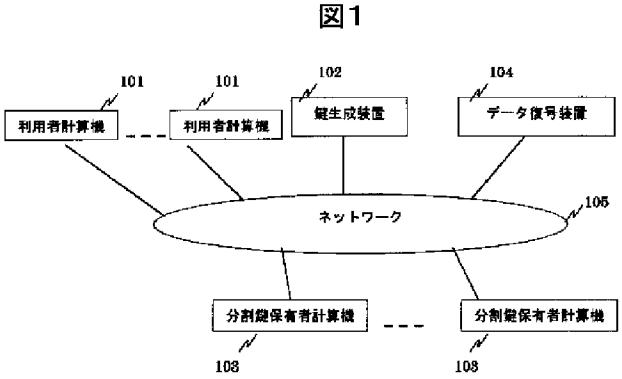
【図２６】第３の実施形態においてデータの復号手順の詳細を示すフローチャートである。

【図２７】第３の実施形態において表示部に表示されるファイルオープン選択画面の例を示す図である。

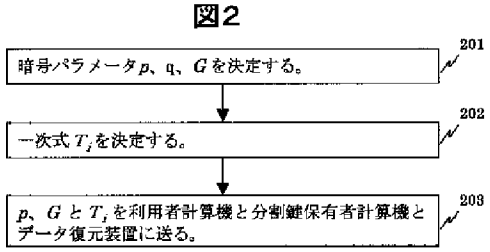
【符号の説明】

１０１…利用者計算機、１０２…鍵生成装置、１０３…分割鍵保有者計算機、１０４…データ復号装置、１０５…ネットワーク、１１２－１～１１２－N…供託機関計算機。

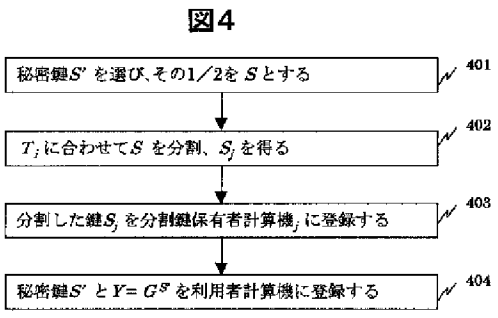
【図１】



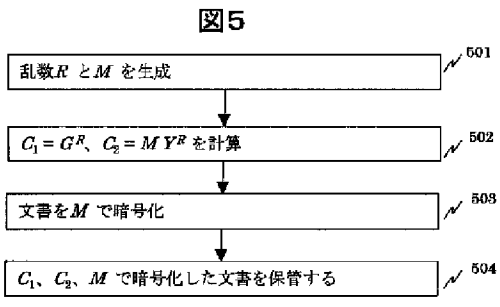
【図２】



【図４】

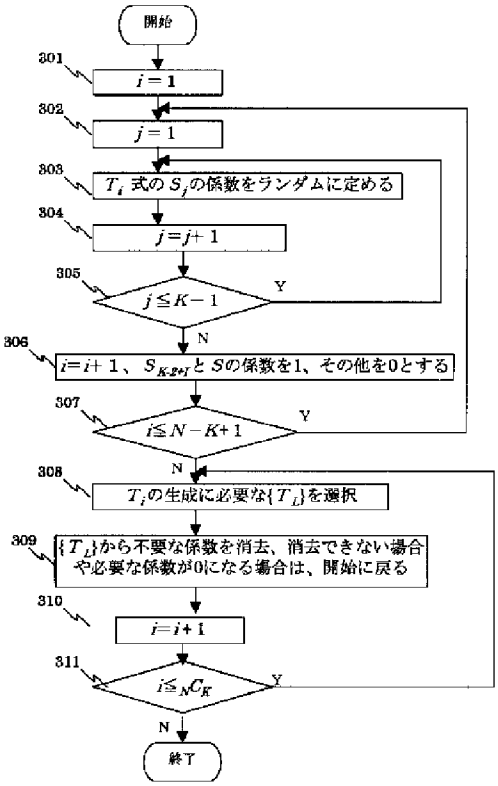


【図５】



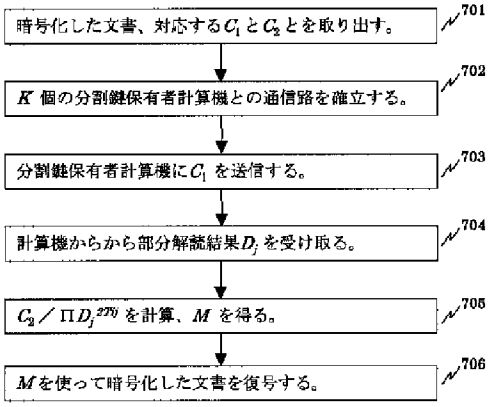
【図３】

図3



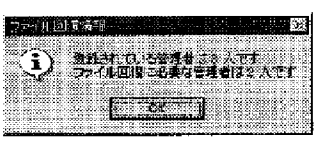
【図７】

図7



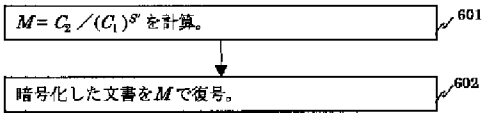
【図１９】

図19



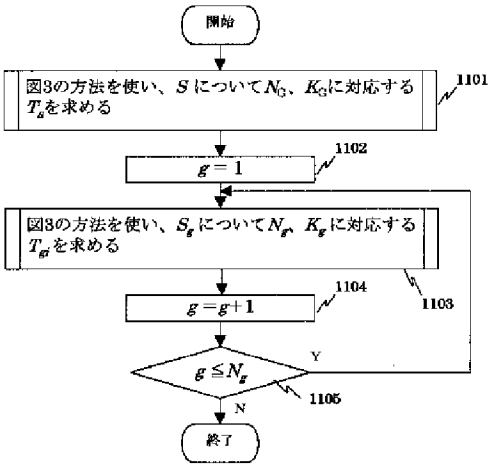
【図６】

図6



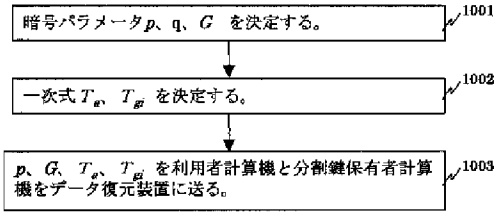
【図１１】

図11



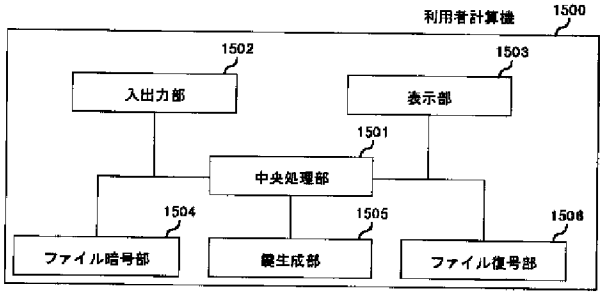
【図１０】

図10



【図１５】

図15



【図８】

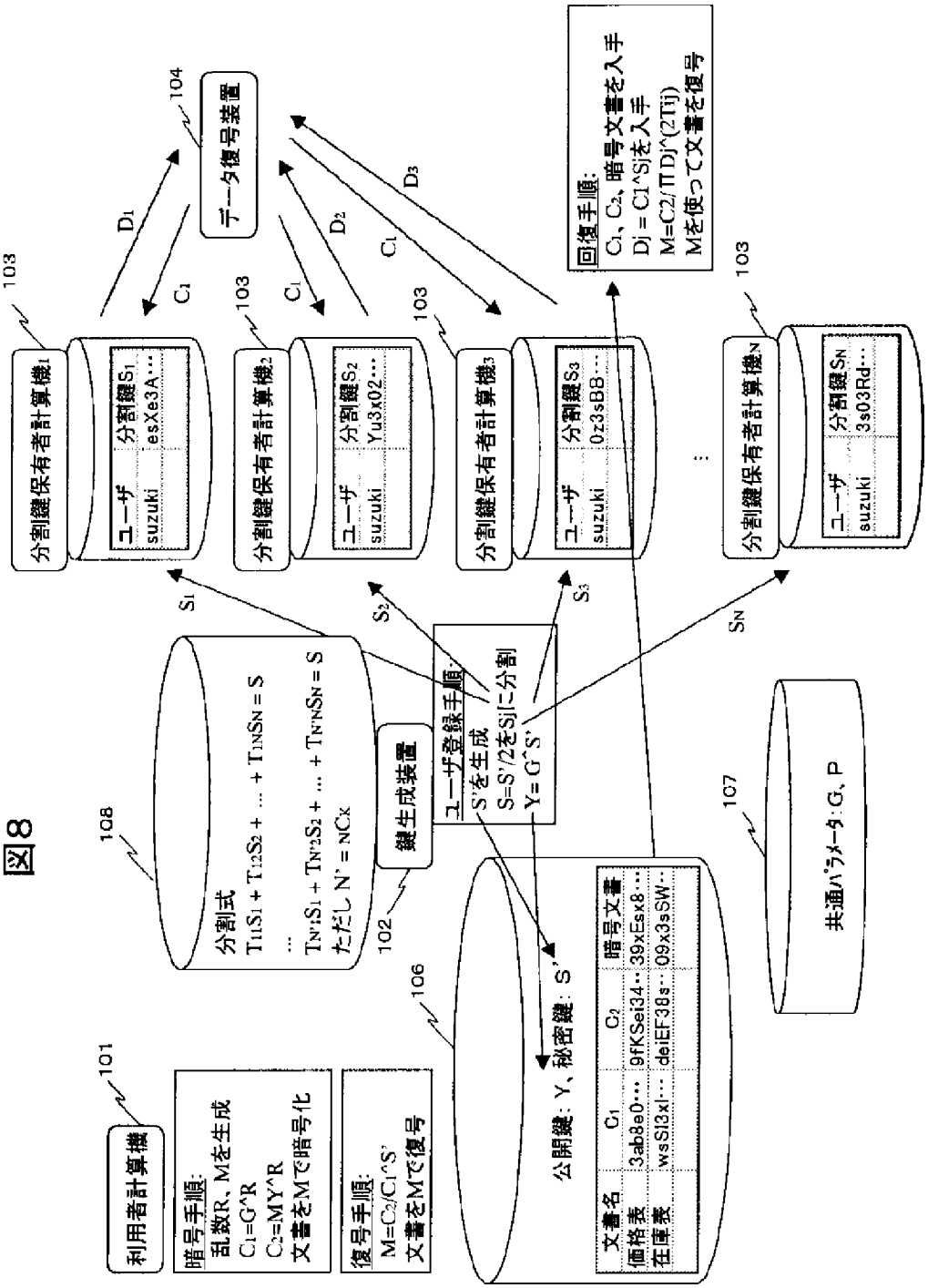


図8
利用者計算機
101
暗号手順:
乱数R、Mを生成
C1=G^R
C2=MY^R
文書をMで暗号化
復号手順:
M=C2/C1^S'
文書をMで復号
分割式
T11S1 + T12S2 + ... + T1NSN = S
...
TN1S1 + TN2S2 + ... + TNNSN = S
ただし N' = NCk
108
102
鍵生成装置
ユーザ登録手順:
S'を生成
S=S'/2をSjに分割
Y= G^S'
公開鍵: Y、秘密鍵: S'
106
文書名 C1 C2 暗号文書
価格表 3ab8e0… 9fKSei34… 39xEsx8…
在庫表 wsSl3xl… deiEF38s… 09x3sSW…
共通パラメータ: G、P
107
分割鍵保有者計算機1
103
ユーザ 分割鍵S1
suzuki esXe3A…
分割鍵保有者計算機2
103
ユーザ 分割鍵S2
suzuki Yu3x02…
分割鍵保有者計算機3
103
ユーザ 分割鍵S3
suzuki 0z3sBB…
分割鍵保有者計算機N
103
ユーザ 分割鍵SN
suzuki 3s03Rd…
データ復号装置
104
D1
C1
D2
C1
D3
C1
S1
S2
S3
SN
回復手順:
C1、C2、暗号文書を入手
Dj = C1^Sjを入手
M=C2/ΠDj^(2Tij)
Mを使って文書を復号

【図９】

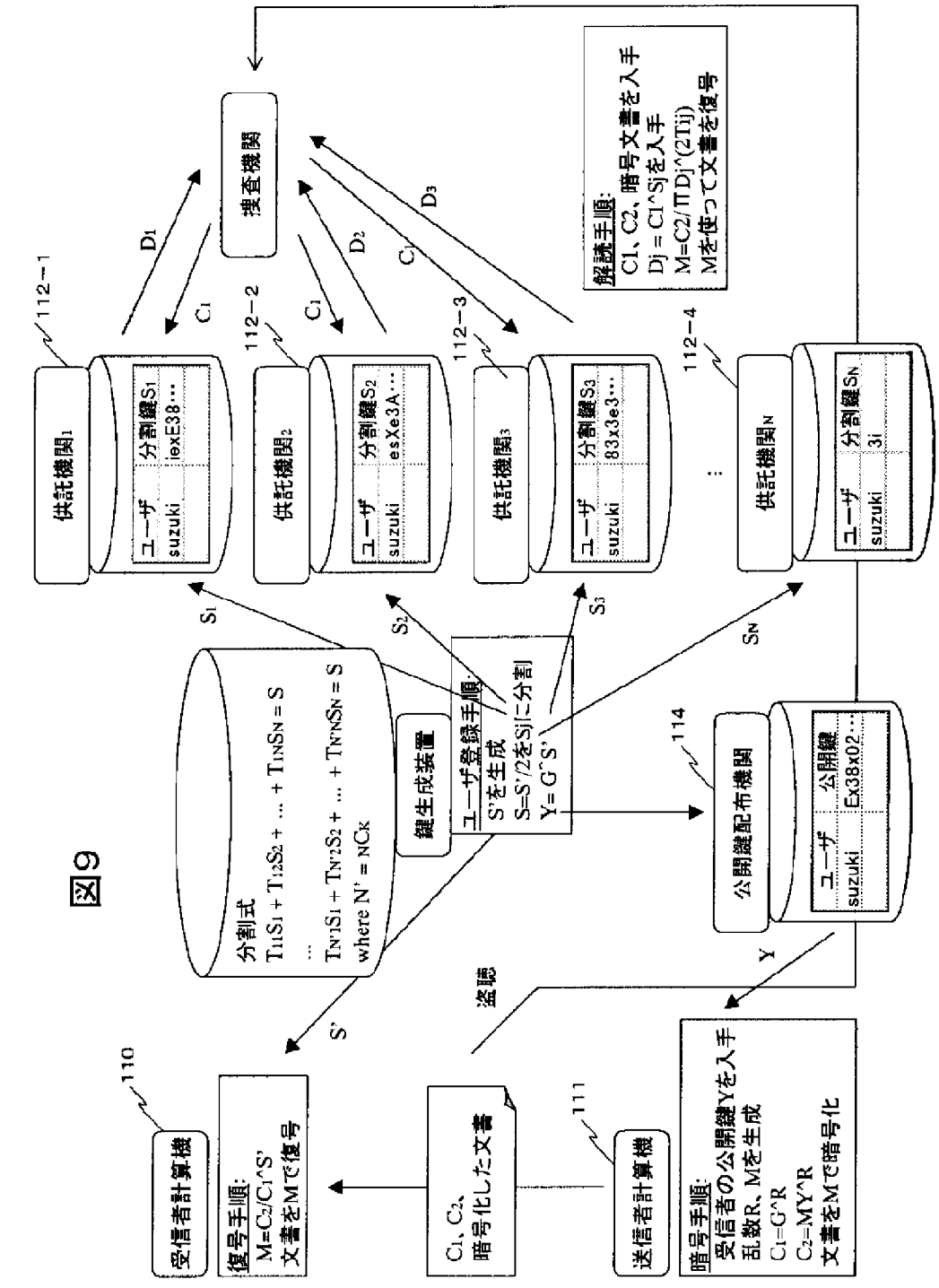
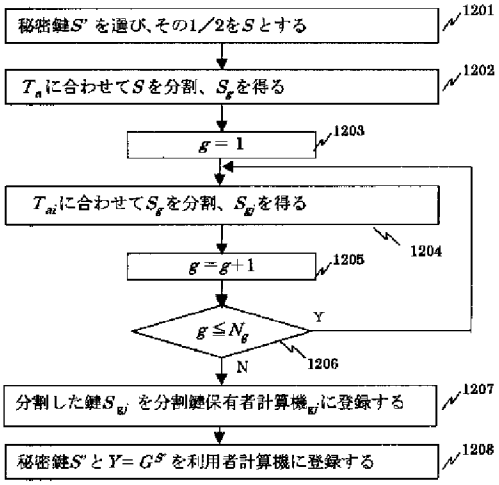


図9
捜査機関
D1
D2
D3
C1
C2
C3
解読手順:
C1、C2、暗号文書を入手
Dj = C1^Sj を入手
M=C2/ΠDj^(2Tij)
Mを使って文書を復号
112−1
112−2
112−3
112−4
供託機関1
供託機関2
供託機関3
供託機関N
ユーザ
分割鍵S1
分割鍵S2
分割鍵S3
分割鍵SN
suzuki
S1
S2
S3
SN
分割式
T11S1 + T12S2 + ... + T1NSN = S
...
TN1S1 + TN2S2 + ... + TNNSN = S
where N' = NCk
鍵生成装置
ユーザ登録手順:
S'を生成
S=S'/2をSjに分割
Y= G^S'
公開鍵配布機関
公開鍵
Ex38x02…
S'
盗聴
Y
110
111
114
受信者計算機
復号手順:
M=C2/C1^S'
文書をMで復号
C1、C2、
暗号化した文書
送信者計算機
暗号手順:
受信者の公開鍵Yを入手
乱数R、Mを生成
C1=G^R
C2=MY^R
文書をMで暗号化

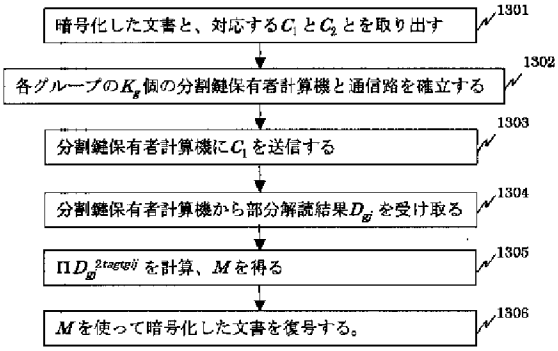
【図１２】

図12



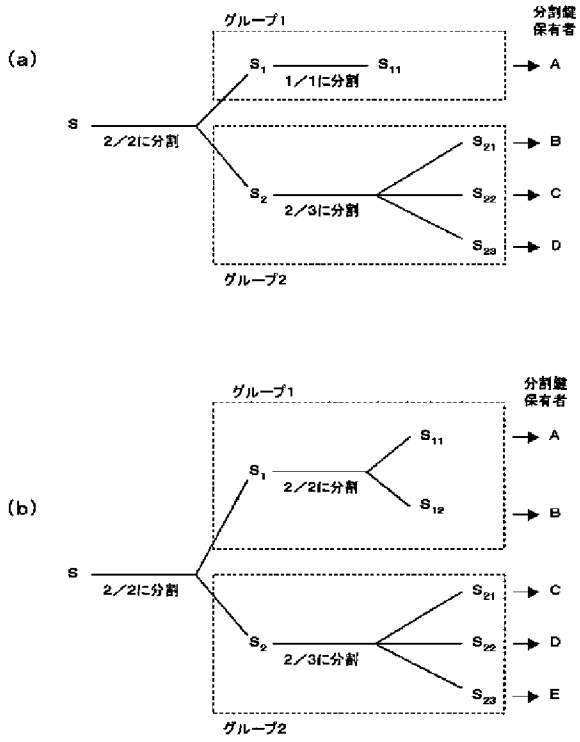
【図１３】

図13



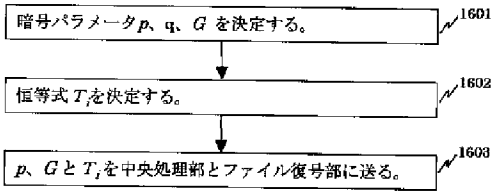
【図１４】

図14



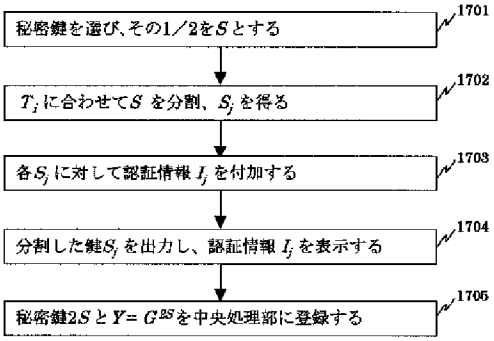
【図１６】

図16



【図１７】

図17

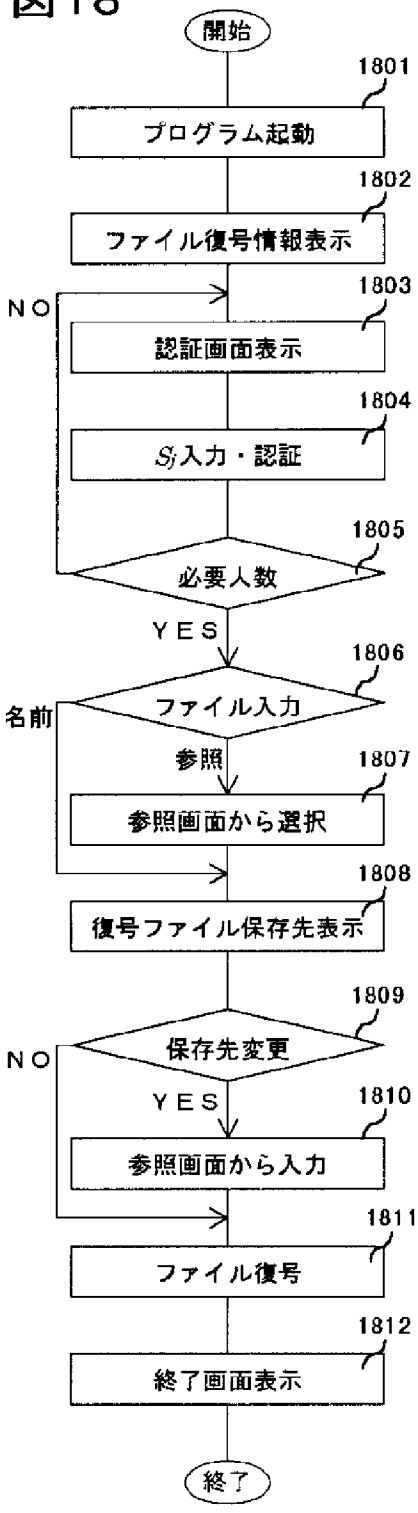


【図２０】

図20

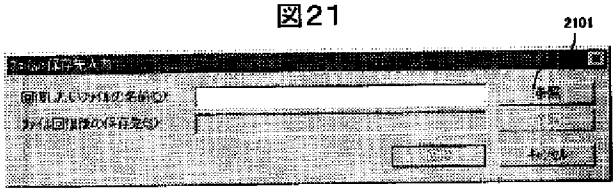
【図１８】

図18



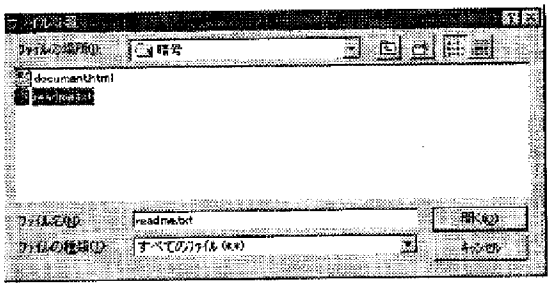
【図２１】

図21



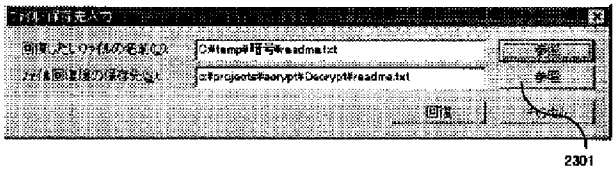
【図２２】

図22



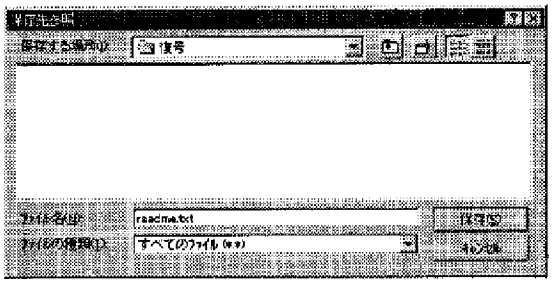
【図２３】

図23



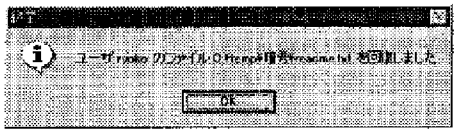
【図２４】

図24



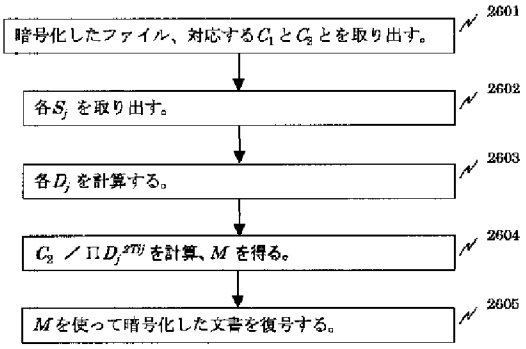
【図２５】

図25



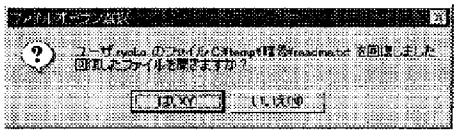
【図２６】

図26



【図２７】

図27



フロントページの続き

(72)発明者　宮崎　博
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会
社内

(72)発明者　遠田　潤一
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会
社内